(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/17310 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 29/06

(21) International Application Number: PCT/SE00/01673

(22) International Filing Date: 31 August 2000 (31.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/386,253 31 August 1999 (31.08.1999) US

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: MARIZ RIOS, José Luis; Bronce 37, 4-19, E-28045 Madrid (ES). RUIZ SANCHEZ, José Luis; Rosas de Aravaca 82F-2D, E-28032 Madrid (ES).

(74) Agent: ERICSSON RADIO SYSTEMS AB; Common Patent Department, S-164 80 Stockholm (SE).

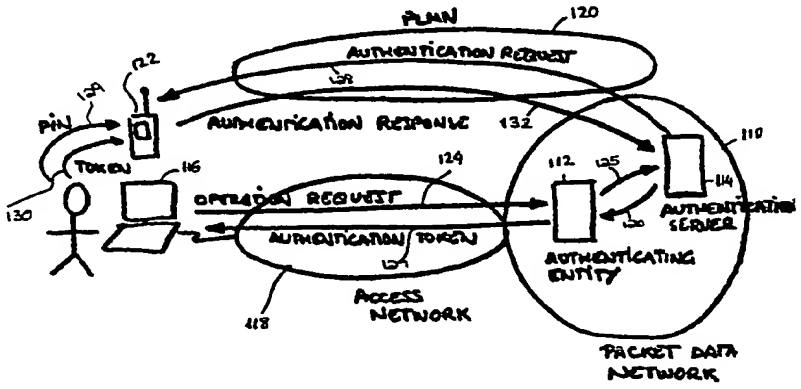
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: GSM SECURITY FOR PACKET DATA NETWORKS



(57) Abstract: In a communication system methods and apparatus that apply GSM security principles to authenticate users who are requesting access to packet data networks are provided. The authentication process is triggered by an authenticating entity when it needs to verify the identity of a user trying to access certain resources, e.g., an application of a network. The authenticating entity sends an authentication request to an authentication server. The authentication server checks whether the user's identity corresponds to a known user. If so, the authentication server generates an authentication token that is sent to the user via an access network and a remote host. The authentication server uses a secure communication link, via a wireless network, to request the user to send the authentication token back to the authentication server via the secure communication link over a public land mobile network. Once the user sends the authentication token back to the authentication server via the secure channel, the authentication server compares the authentication token sent to the user and received from the user through the secure communication link. If the authentication tokens match, the authentication server instructs the authenticating entity to grant the user access to the requested services. If the authentication tokens do not match, the user will be denied access to the requested services.

WO 01/17310 A1

GSM SECURITY FOR PACKET DATA NETWORKS

BACKGROUND

The present invention relates generally to methods and apparatus for providing security for packet data networks and more particularly methods and apparatus that apply GSM security principles to authenticate users who are requesting access to packet data networks.

The number of users who access Packet Data Networks (PDN), e. g., the Internet, from remote locations increases each day. Thus, the number of private networks that are interconnected to the Internet has grown significantly. A private network is typically a network in which access to host sites of the private network is limited to authorized users. When the private network is connected to the Internet, security procedures, including authentication procedures, are carried out to ensure that only authorized users from authorized hosts can gain access to the private network. For example, when a user requests access to a host site of the private network from a remote location, the user must be authenticated before the user is granted access to the host site.

Some conventional authentication procedures use passwords. A password is a string of characters recognized by automatic means and permits a user access to protected files, or input or output devices. Most sophisticated systems, such as Kerberos, use authentication schemes based on passwords. Kerberos is a security system for client/server computing.

A password may be generated at a remote site, which is requesting access to a host site of the private network. Some systems utilize either symmetric or asymmetric cryptographic techniques to create and authenticate the password, which will be described in detail later.

The continuous development of PDNs has generated a wide range of computer services. In some cases, the services are restricted to a number of users. In other cases, the services are dynamically accessed on a commercial basis, i.e., the users pay to utilize the services. In both of the above-mentioned cases, the users must authenticate themselves using a service provision system of a service provider before they can gain access to the desired services. Thus, the service provider ensures that only users entitled

to access the services can do so.

Cellular communication systems control resources of a network that are utilized by Mobile Stations (MS) corresponding to authorized users. In a conventional GSM cellular communication system the MS includes a Subscriber Identity Module (SIM). The SIM contains subscriber information including, for instance, data used to permit the MS to gain access to the network infrastructure of the GSM cellular communication system. The SIM participates in the authentication of the user and in the subsequent encryption, if any, of a radio communication.

A user identity authentication operation verifies that service is provided only to a limited and controllable set of users, whereas the authorization operation verifies that a limited and controllable set of resources are provided to the proper users. In principle, getting access to a network is similar to getting access to any particular application server in the sense that it requires a client opening a session with a specific server, e.g., the access server. The access session embraces all other possible sessions with different servers, and it is a requirement prior to any interaction with a server in the network. Each server can have its own procedures for authenticating and authorizing users.

Remote access to public or private data networks is growing tremendously, especially through dial-up PSTN/ISDN connections, which are unsafe, because they transmit data over unsecured communication lines. Additionally, software for security breaking is quite advanced and more widely used than it was in the past, which makes it more difficult to prevent unauthorized users from getting access to secured information.

Since data networks are growing rapidly, separate security procedures for each application of the data network might not be enough to protect against an intruder once the intruder places himself into the data network. Thus, overall data network security procedures and policies are becoming more necessary to protect private packet data networks.

Weak authentication and strong authentication are two commonly known types of authentication. Both weak and strong authentication may use known authentication security methods such as: a token (e.g., a unique combination of bits), a password (e.g., a secret character string), or biometric information (e.g., fingerprint, voice print, retinal scan, etc.).

Weak authentication is referred to as single-factor authentication, because it uses a single method to authenticate a user. Weak authentication also encompasses techniques including traditional static passwords and one-time passwords. Static passwords, however, can be broken by software programs, including keyboard strike monitoring programs, cracking programs for guessing, and network sniffing programs.

Static passwords can be protected from the above-mentioned software programs by generating a one-time password (one per session) that can not be calculated from previous passwords, i.e., introducing a pseudo-random sequence as a calculation factor. The one-time password is generated from a "real" password that would never be transmitted over the network (a shared secret between the user and the network).

Strong authentication is referred to as two-factor authentication. Strong authentication is safer than weak authentication because it authenticates the user by using two methods, normally a token and a password. Systems that generate one time pass-codes from a token and a password are already available in the market, such as Security Dynamic's Secure ID, Safeword's Safeword DES Gold Card and Digital Pathway's Defender. For example, the token may be a hardware device and the password may be a Personal Identification Number (PIN) code to access the hardware device.

Strong authentication still can be made safer, for example, by introducing explicit authentication, the network generates a random factor as input to the user's password generation operation (this is known as that the network challenges the user). Second, the life cycle of the pass-code can be very short, e.g., 1 minute, therefore implementing a continuous authentication process as the session goes on. Third, more sophisticated keys and algorithms, based either in symmetric or asymmetric cryptography, can be used.

The most commonly used authentication procedures are based on identity/password methods. Most advanced systems utilize one-time passwords and token-based methods. However, those implementations have limitations. For example, static login/password methods provide weak security. Additionally, strong authentication methods require a user to hold additional devices, i.e., token devices. Some strong authentication mechanisms require specific hardware, e.g., smartcard readers. Furthermore, some strong authentication methods require specific hardware and software configurations that result in an administrative burden. Accordingly, lack of flexibility of

the token devices creates further problems with strong authentication methods.

Thus, there is a need to apply GSM security principles to authenticate users in PDNs in order to improve security in accessing private service networks as well as specific services and applications of such private service networks.

There is a further need to use two different communication channels between a private service network and a user requesting access to it, wherein one of the channels would be an unsecured channel connected to a PDN over an access network and would not carry any sensitive information between a remote host and the PDN, and the other channel would be a secured channel that would exchange security information between a MS and the PDN over a Public Land Mobile Network (PLMN). There is a further need to use such GSM security principles to authenticate a user when performing e-commerce transactions.

SUMMARY

According to Applications' invention, these and other objects are met by methods and apparatus that apply GSM security principles to user authentication in PDNs in order to improve access security to private service networks.

According to an exemplary embodiment of the present invention, a communication system for authenticating a user requesting access to a PDN comprises a PLMN connected to the PDN. A remote host is connected to the PDN via an access network. A mobile station maybe coupled to the PLMN via a wireless link. In response to the user requesting access to the PDN, the PDN generates and sends an authentication token over an unsecured or secured communication channel to the user via the access network and the remote host. The user sends the authentication token back to the PDN over a secured channel of the PLMN, wherein the PDN compares the authentication tokens to determine whether to grant the user access to the PDN.

According to another exemplary embodiment of the present invention, a communication system has an e-commerce server that authenticates a user when performing an e-commerce transaction. A user who wishes to perform an e-commerce transaction sends a request to the PDN. The PDN generates an authentication token. A payment server that handles the charging aspect for an e-commerce application is

contacted. The authentication token is sent to the user from the PDN via an access network using an unsecured or secured communication line. The user sends the authentication token back to the PDN via a secured communication channel over a PLMN. The authentication token that was sent to the user is compared to the authentication token that is sent by the user to the PDN to determine whether the user is authorized to proceed. The communication system also has an authentication server that communicates with the payment server to charge the user for the e-commerce transaction. Additionally, billing information may be sent to a billing system of the PLMN.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become apparent by reading this description in conjunction with the accompanying drawings, in which like reference numerals refer to like elements and in which:

FIG. 1 is a block diagram that illustrates a communication system according to an exemplary embodiment of the present invention;

FIG. 2 is a block diagram that illustrates a mobile station structure according to an exemplary embodiment of the present invention;

FIG. 3 is a block diagram that illustrates a method of authenticating a user according to an exemplary embodiment of the present invention;

FIG. 4 is a flow chart that illustrates a method of communicating between Mobile Equipment (ME) and a SIM of a MS according to an exemplary embodiment of the present invention;

FIG. 5 is a block diagram that illustrates a communication system for authenticating the user when accessing a PDN in a dial-up scenario according to another exemplary embodiment of the present invention;

FIG. 6 is a message sequence chart illustrating a method of authenticating a user according to another exemplary embodiment of the present invention;

FIG. 7 is a block diagram that illustrates a communication system for authenticating the user when performing e-commerce transactions according to an exemplary embodiment of the present invention;

FIG. 8 is a message sequence chart that illustrates a method of authenticating the

user when performing e-commerce transactions according to an exemplary embodiment;

FIG. 9 is a block diagram that illustrates a communication system that uses Unstructured Supplementary Service Data (USSD) according to an exemplary embodiment of the present invention;

FIG. 10 is a message sequence chart that illustrates a method of authenticating a user in a network scenario using USSD according to an exemplary embodiment of the present invention;

FIG. 11 is a block diagram that illustrates a communication system that uses a Wireless Application Protocol (WAP) according to an exemplary embodiment of the present invention; and

FIG. 12 illustrates a method of authenticating a user in the communication system shown in FIG. 11.

DETAILED DESCRIPTION

FIG. 1 is a block diagram that illustrates a communication system according to an exemplary embodiment of the present invention. In FIG.1, the communication system comprises a PLMN 22, a PDN 24, an access network 26, a remote host 32 and a MS 68.

The PDN 24 may be connected to access network 26 via communication links (not shown). Access network 26 may be connected to the remote host 32 via a communication link 30.

The PLMN 22 comprises a Base Transceiver Station (BTS) 36 connected to a Base Station Controller (BSC) 38 via a communication link 40. A Mobile Switching Center/Visitor Location Register (MSC/VLR) 42 may be connected to both the BSC 38 and a Short Message Service Center (SMS-C) 44 via communication links 46 and 48, respectively. A Home Location Register (HLR) 50 may be connected to the MSC/VLR 42 and an Authentication Center (AuC) 52 via communication links 54 and 56, respectively.

The PDN 24 comprises an authentication server 58 connected to an authenticating entity 60 via a communication link 62. A WAP server 76 maybe connected to the authentication server 58 via communication link 78. A Network Access Service (NAS)/Router 64 is connected to the authenticating entity 60 via communication link 66.

The authentication server 58 may be connected to the SMS-C 44 via communication link 72. The detailed aspects of this connection are not critical to the present invention, and therefore are not shown. However, the connection depends on the type of connection (e.g., X.25, IP) and the security mechanisms in place (e.g., IPsec. tunnel servers, routers, firewalls). The HLR 56 may be connected to the authentication server 58 via communication link 74.

The MS 68 communicates with the PLMN 22 via a wireless connection, shown as radio link 70.

The PLMN 22 may be constructed according to the Global System for Mobile Communication (GSM) standard described in European Telecommunication Standard Institute (ETSI) documents ETS 300 573, ETS 300 574 and ETS 300 578, which are hereby incorporated by reference. The GSM specification is known in the art and thus will not be described further herein. The BTS 36 receives uplink signals generated by the MS 68 via the radio link 70. The BTS 36 generates downlink signals to transmit to the MS 68 via the radio link 70. The BTS 36 also communicates with the BSC 38, which controls the operation of a group of base stations (not shown).

The HLR 50 contains subscription and location information regarding subscribers to the communication system. The HLR 50 is thus used to identify/verify a subscriber. The HLR 50 also contains subscriber data relating to features and services of the communication system available to the subscriber. The AuC 52 handles the security functionality for the PLMN 22. The AuC 52 stores the subscriber's private keys and applies A3 (authentication) and A5 (ciphering/deciphering) security algorithms. The A3 and A5 security algorithms are described in ETSI document ETS 300 929, which is hereby incorporated by reference. The A3 and A5 algorithms are also specified in appendix C of ETS 300 534, which is hereby incorporated by reference.

The SMS-C 44 receive messages generated at the PDN 24 via the communication link 72. The SMS-C 44 packs the received messages into Short Message Service (SMS) messages. The SMS messages are transmitted as defined in the corresponding GSM standard specification and thus will not be further described herein.

The remote host 32, e.g., a personal computer or laptop computer, contains conventional client software for remote access to the PDN 24, such as, Microsoft's

Internet Explorer, America On-Line's Netscape Navigator, etc.

The PDN 24 comprises many hosts (all not shown). The authenticating entity 60 is responsible for ensuring that only authorized users are given access to resources in the PDN 24. These resources may include applications or content within applications. It will be appreciated by those of ordinary skill in the art that the PDN 24 and the access network 26 may be connected through intermediate PDNs, e.g., ISP, Intranets. It will also be appreciated by those of ordinary skill in the art that the access network 26 may be a cellular network, and thus would link the remote host 26 to the NAS/Router 64 via conventional wireless methods. It will also be appreciated by those of ordinary skill in the art that the authentication server 58 may be connected to the PLMN 22 via an intermediate gateway system.

The authentication server 58 provides authentication service to the PDN 24. The authentication server 58 generates an authentication token for each access request and handles the dialogue with the authentication application in a processing device (not shown) of the MS 68. The processing device will be described in detail later with the description of FIG. 2. The authentication server 58 validates the response from the processing device. The authentication server 58 communicates the result of the authentication process to the authenticating entity 60. Any possible encryption of communication between the processing device and the authentication server 58 requires that the corresponding algorithms and key values be stored in the authentication server 58. If the GSM security scheme is re-used, the authentication server 58 will neither store the keys itself nor calculate the authentication algorithms, rather it will obtain the necessary values from the corresponding AuC 52 in the GSM network. When the authentication is associated to a payment, the authentication server 58 is responsible for establishing the corresponding dialogue with a payment server (not shown) and forwarding the necessary information (e.g., prices) from the authenticating entity to the payment server.

The authenticating entity 60 invokes the appropriate mechanisms, e.g., protocols application programming interfaces, to request authentication from the authentication server 58. The authenticating entity 60 forwards an authentication token to the remote host 32 and processes the outcome of the authentication process. When authentication is

associated with an operation that requires the recording of additional information, e.g., a payment, the authenticating entity 60 requests user authentication via the authentication server 58. The authentication request includes the additional information.

It will be appreciated by those of ordinary skill in the art that the authenticating entity 60 and the authentication server 58 may be located in different PDNs, provided they are linked by a secure data channel, e.g., IPsec. tunnel.

FIG. 2 is a block diagram of a mobile station structure and the network environment interacting with it in a scenario using SMS, according to an exemplary embodiment of the present invention. The mobile station structure (MS) 80 comprises a SIM 90 and ME 92. The network environment comprises a PLMN 82, and an authentication server 84. The PLMN 82, in turn, comprises a SMS-C 86 that may be connected to the authentication server 84 via communication link 88.

The ME 92 comprises a keypad 102 and a display 104. The SIM 90 comprises a SIM operating system (SIM OS) 96, a GSM part 98, a SIM Application Toolkit (STK) 100, and an authentication application, i.e., a processing device, shown as AUTH-APP 108. The ME 92 and the SIM 90 communicate with each other via a communication link 94.

The SIM 90 may be a "smart" card installed into the MS 80 and contains subscriber information including, for instance, data used to permit the MS 80 to gain access to the network infrastructure of the GSM communication system. The SIM 90 participates in the authentication of the user and in the subsequent encryption of the radio communication, if any.

The MS 80 communicates with the PLMN 82 via a wireless communication link, shown as radio link 106.

The SIM 90 is compliant with the standards of the ISO/EEC/7816 and GSM 11.14 (Phase 2+) specification. GSM 11.14 defines the interface between the SIM 90 and the ME 92, and mandatory procedures for the ME 92, specifically for the AUTH-APP 108. The AUTH-APP 108 is a framework for enabling the applications existing in the SIM 90 to interact and operate with the ME 92. For example, interactions include displaying messages on the display 104, obtaining a user's input from the keypad 102 and sending and receiving short messages via the radio link 106.

The SIM OS 96 provides for the execution and management framework for the GSM application that handles the conventional GSM functionality. Together with it, the STK 100 provides the environment for all kinds of applications like the AUTH-APP 108.

The AUTH-APP 108 handles the communication with the authentication server 84 through a secure channel (not shown). When the AUTH-APP 108 receives an authentication request from the authentication server 84 via the PLMN 82, it instructs the MS 80 to request an authentication token. Once the authentication token has been input into the MS 80, the AUTH-APP 108 sends the authentication response containing the authentication token back to the authentication server 84 via the PLMN 82. The execution of the authentication application performed by the AUTH-APP 108 may be protected by a PIN code. Any possible encryption of the communication between the AUTH-APP 108 and the authentication server 84 requires that the corresponding algorithms and key values be stored in the AUTH-APP 108.

Still referring to FIG. 2, a higher security level can be achieved by the use of end-to-end encryption in the communication path between the MS 80 and an authentication server 84. Encryption takes place at the application level between the AUTH-APP 108 of the MS 80 and at the authentication server 84.

Encryption of the data contents exchanged by the MS 80 and the authentication server 84 can be achieved according to either symmetric encryption or asymmetric encryption. In symmetric encryption, a secret key is shared between the AUTH-APP 108 of the SIM 90 and the authentication server 84. The secret key is used to encrypt the data at the MS 80 and the authentication server 84. Normally, such secret key for channel encryption (also called ciphering key) is generated per communication session between the two communicating parties (MS 80 and authentication server 84), based on some seed string which normally is the user's individual secret key. Each user is assigned an individual secret key when the user signs up for the services. The user keeps the same key, unless the secret key has to be updated.

In one embodiment of the invention, the user authentication is enhanced by challenging the user's individual secret key stored in the SIM 90. This is done by standard GSM authentication methods, from the authentication server 84 and thus will not be described further herein. The authentication server 84 is connected to the GSM

core network to access the security information from an AuC (not shown) of the PLMN 82. The authentication server 84 does not need to run the GSM encryption algorithm or store the user's secret key. Instead, the authentication server 84 may retrieve a random number (RAND) and SRES pairs for the user from the AuC. The AUTH-APP 108 in the SIM 90 can re-use the GSM security information (key and algorithm); it will use the A3 algorithm to obtain the SRES from the RAND and the individual secret key stored in the SIM 90.

FIG. 3 illustrates a method of authenticating a user according to an exemplary embodiment of the present invention. In FIG. 3, a communication system comprises a remote host 116, an access network 118, a PLMN 120, MS 122, and a PDN 110, which comprises an authenticating entity 112 and an authentication server 114.

In FIG. 3, the method begins at step 124 where a user initiates an operation request to connect the remote host 116 to the PDN 110 via the access network 118. At step 125, authenticating entity 112 communicates with the authentication server 114 via a secure packet data connection (not shown) and requests the authentication of the user trying to gain access to the PDN 110.

At step 126, the authentication server 114 provides the authenticating entity 112 with an authentication token (not shown). At step 127, the authenticating entity 112 transmits the authentication token to the remote host 116 via the access network 118.

At step 128, the authentication server 114 contacts the MS 122 via the PLMN 120, using conventional wireless methods, and requests the user to transmit via the MS 122 the authentication token that was sent to the remote host 116 in step 127 back to the authentication server 114 via the MS 122 and the PLMN 120.

The MS 122 may request the user to input a PIN code before the user can input the authentication token into the MS 122 using an input device such as for example, a keypad. At step 129, the user inputs the PIN code using the keypad of the MS 122. Once the PIN code has been validated, an application in the SIM within the MS 122 communicates with the MS 122 to prompt the user to input the authentication token received by the remote host 116 in step 127. At step 130, the user inputs the authentication token using an input device such as the keypad of the MS 122.

At step 132, the application of the SIM instructs the MS 122 to send the

authentication token back to the authentication server 114 via the PLMN 120. Finally, the authentication server 114 determines if the authentication token received via the PLMN 120 matches the authentication token that was transmitted to the remote host 116 in step 127. If the authentication tokens match, the authentication server 114 instructs the authentication entity 112 to grant the user access to the requested service. If the authentication tokens do not match, an appropriate error condition will be sent to the authenticating entity 112. Thus, the user is denied access to the requested service.

It will be appreciated by those of ordinary skill in the art that the MS 122 and the remote host 116 may be linked via a wireless, wireline, or infrared connection (not shown) to achieve a faster authentication process. For example, the application in the SIM can retrieve the authentication token from the remote host 116 without user intervention as described below.

Referring back to step 129, the user may input the PIN code in the remote host 116 instead of the MS 122. The remote host 116 may then automatically forward the PIN code to the MS 122 via a wireless, wireline, or infrared connection between the MS 122 and the remote host 116. Furthermore, the PIN code could be stored in the remote host 116 where the remote host 116 may automatically transfer the PIN code to the MS 122 via the wireless, wireline, or infrared connection, once the remote host 116 receives the authentication token as described in step 127.

Alternatively, referring back to step 130, the MS 122 may automatically retrieve the authentication token from the remote host 116 via the wireless, wireline, or infrared connection.

FIG. 4 is a flow chart illustrating an exemplary embodiment of the method of communicating between the ME 92 and the SIM 90 of the MS 80 shown in FIG. 2. According to FIG. 4, at step 140, the ME 92 receives a short message from a PLMN 82 (FIG. 2). The short message may be a message requesting the ME 92 to send an authentication token to the PLMN 82. At step 142, the ME 92 sends an authentication request (SMS-PP Download) to the SIM 90. The SIM 90 activates its authentication application, reads the authentication request and obtain a RAND. At step 144, the SIM 90 sends a PIN code request to the ME 90. A user responds to the PIN code request by inputting a PIN code using an input device such as the keypad 102 (FIG. 2) of the ME 92.

The ME 92 may display the inputted PIN code on the display 104. The ME 92 reads the PIN code from the keypad 104.

Next, at step 146, the ME 92 sends the PIN code to the SIM 90. The SIM 90 checks the PIN code to verify that it is an authorized PIN code for the ME 92. The SIM 90, then at step 148, sends an authentication token request to the ME 92. The user responds by inputting the authentication token using an input device such as the keypad 108. The ME 92 may display the inputted authentication token on the display 104 and reads the authentication token from the keypad 102. The ME 92, at step 150, sends the authentication token to the SIM 90. The SIM 90 calculates the SRES applying the A3 security algorithm to the RAND and private key. The SIM 90 prepares a response using SRES and the authentication token. At step 152, the SIM 90 sends an authentication response to the ME 92. Finally, at step 154, the ME 92 sends a short message, which contains the authentication token, to the PLMN 82.

Referring back to FIG. 3, the application within the SIM in the MS 122 may securely store an authentication key, as well as the authentication server 114. Optionally, keys can be generated and/or stored within the authentication server 114. The keys may also be obtained from an external node providing suitable generation and/or storage functionality.

It will be appreciated by those of ordinary skill in the art that a session key could be used in the encryption of the subsequent communications between a remote host and an authenticating entity in a PDN. A session key could be obtained applying an appropriate algorithm to the RAND and using the private key. This is done, for instance in the GSM system during the calculation of the ciphering key (Kc), where an A8 security algorithm is applied to RAND using the subscriber's private key. The Kc generating algorithm is called the A8 security algorithm and is used to compute the Kc from the RAND sent during the authentication procedure. The A8 algorithm is operator specific. The A8 is applied at the PLMN 120 by the AuC (not shown) and at the user side by the SIM (not shown) in the MS 122. Thus the Kc does not have to be transmitted, since it is calculated at both ends of the encrypted channel. The specification for the A8 algorithm is described in appendix C of the ETS 300 534, which has previously been incorporated by reference.

In this approach, the application in the SIM (not shown) of the MS 122 could apply the appropriated algorithm to obtain a session key on reception of the authentication token. Then it would send the resulting session key to the dial-up client in the remote host 116 via the MS 122. The dial-up client may apply the received key for the encryption/decryption of the subsequent communications with the PDN 110.

The authentication server 114 would also obtain the session key applying the same algorithm that the application in the SIM of the MS 122 used to calculate the session key. The authentication server 114 may also include the session key in the authentication response sent to the authenticating entity 112.

When asymmetric encryption is used to generate the session key at the authentication server 114, it is encrypted with the subscriber's public key, and sent along with the RAND in the message to the application in the SIM of the MS 122. The application in the SIM of the MS 122 may obtain the session key value using its private key. Then it may send the resulting session key to the dial-up client in the remote host 116 via the MS 122. The dial-up client may apply the received key for the encryption/decryption of the subsequent communications with the PDN 110. The SIM in the MS 122 will store its own private key and the public key of the authentication server 114. Thus, the authentication server 114 will store its own private key and the public keys of each user. Optionally, the authentication server 114 could retrieve those keys from an external node (not shown).

The discussion below describes a unilateral two-pass authentication mechanism. Other mechanisms, such as the ones shown in ISO/IEC 9798-3, may be also applicable, including mutual authentication.

Still referring to FIG. 3, assuming that the authentication server 114 stores the necessary keys and it is able to apply the encryption algorithm, the user initiates connection by means of a remote host 116 to an access server in a PDN 110. The access network provides the communication path between the remote host 116 and to the PDN 110.

The authentication entity 112 contacts the authentication server 114 via a secure packet data connection and requests the authentication of the user trying to gain access. The authentication server 114 generates a RAND. Then, it contacts the MS 122 using a

wireless network infrastructure. The message includes the RAND.

The authentication server 114 provides the authentication entity 112 with an authentication token that is forwarded to the remote host 116 via the access network 148.

The application in the SIM of MS 122 receives the message from the authentication server 114 according to the usual wireless procedures.

The application in the SIM of MS 122 optionally communicates with the MS 122 to require the user to introduce a PIN code. Once the PIN code has been validated, the application communicates with the MS 122 to request the user to introduce the authentication token received by the remote host 116. The application constructs the authentication response message including the signature corresponding to the received RAND applying the algorithm (symmetric or asymmetric) to RAND using the key stored in the SIM in the MS 122. The signature may optionally include the authentication token.

The application in the SIM of MS 122 instructs the wireless terminal to send the response back to the authentication server 114 using standard wireless procedures.

Finally, the authentication server 114 determines if the response received via the wireless network is correct and includes the authentication token. The authentication server 114 will apply the algorithm (symmetric or asymmetric) to the received signature using the key for that user. If the resultant information matches the RAND and authentication token values, the authentication server 114 instructs the authentication entity 112 to grant the user access to the requested service. Otherwise, an appropriate error condition is sent to the authenticating host.

The present invention is well suited for dial-up access authentication for a communication system. FIG. 5 is a diagram of a communication system according to another exemplary embodiment of the present invention. In FIG. 5, the communication system comprises a PLMN 160, a PDN 162, a remote access network 164, a modem 166, a remote host 170 and a MS 208. The MS 208 communicates with the PLMN 160 via a wireless link shown as radio link 210. The PLMN 160 comprises a BTS 172, BSC 174, a MSC/VLR 178, a SMS-C 180, a HLR 186 and an AuC 188. The PDN 162 comprises an authentication server 194, an authentication, authorization and accounting (AAA) server 196, and a NAS 200. The communication system of FIG. 5 is substantially similar to the communication system of FIG. 1, except the authentication entity 60 of FIG. 1 is replaced

with the AAA server 196 of FIG. 5. The NAS 200 communicates with the AAA server 196 using a suitable protocol, e.g., RADIUS.

The authentication server 194 acts as a back-end server for the AAA server 196. The AAA server 196 receives an authentication request from the NAS 200 for a user who is configured to use the communication system. With the exception of the AAA server 196, the components of FIG. 5 perform the same function as their corresponding components of FIG. 1, and thus will not be described further herein.

FIG. 6 is a message sequence chart illustrating a dial-up scenario of the communication system of FIG. 5 according to an exemplary embodiment of the present invention. The protocols used in FIG. 6 are solely for illustrative purposes and thus do not limit the applicability of the present invention.

The user starts the communication from the User PC 170, which serves as the user's remote access, to the ISP/Intranet (not shown) using a conventional dial-up client application. Once the communication path to the NAS 200 has been established, the set-up process begins. At step 220, the NAS 200 sends an identity request to the User PC 170, requesting the User PC 170 to identify the user. At step 222, the User PC 170 responds to the identity request by sending a response containing the user's identity to the NAS 200. Once the user identity arrives at the NAS 200, at step 224, an access-request (identity) is sent to the AAA server 196. The AAA server 196 checks the identity of the user and forwards the access-request to the authentication server 194 (step 226).

At step 228, the authentication server 194 obtains a RAND and SRES pair from the AuC 188 in the PLMN 160 (FIG. 5). Then, at step 230 the authentication server 194 requests that the SMS-C 180 generate a SMS message, which requests the application in the SIM (not shown) of the MS 208 to authenticate the user. The request contains the RAND obtained from the AuC 188.

The authentication server 194 checks the user identity it received in step 226 and generates an authentication token. At step 232, the authentication token is sent to the AAA server 196. The AAA server 196 forwards the authentication token to the User PC 170 via the NAS 200, shown as steps 234 and 236. The authentication token is displayed to the user on a display screen of the User PC 170.

At step 238, the MS 208 receives the SMS message containing the RAND and

forwards it to the authentication application of the SIM (not shown) of the MS 208. The authentication application processes the message and requests the user's PIN code, which may be the SIM's PIN code. The user inputs the PIN code using an input device such as keypad of the MS 208 at step 239. The authentication application of the SIM validates the PIN code. If the user types in an incorrect PIN code, the user has a limited number of re-tries to input the correct PIN code. If a maximum number of consecutive failures is reached, the application prevents the SIM from accepting a PIN code. If the PIN code corresponds to the PIN code stored in the SIM, the authentication application prompts the user for the authentication token.

Still referring to step 239, the user enters the authentication token, which may be displayed on the display of the User PC 170 (at step 236), using the keypad of the MS 208. The authentication application applies the appropriate algorithm to the RAND to obtain SRES. The algorithm utilized may be the GSM A3 authentication algorithm, which obtains a SRES from the RAND and a private key stored in the SIM. Then at step 240, the MS 208 sends a short message containing the authentication token and the SRES to the SMS-C 180 based on a request by the authentication application.

At step 242, the User PC 170 sends a response to the NAS 200. The NAS 200, at step 244, sends an access-request response to the AAA server 196. At step 246, the AAA server 196 sends an access-request response to the authentication server 194. Next, at step 248, the SMS-C 180 sends a SMS indication message, which contains the authentication token and the SRES to the authentication server 194.

Once the SMS indication message arrives at the authentication server 194, the authentication server 194 compares the authentication token received to the authentication token sent to the AAA server 196, and the SRES to the SRES obtained from the AuC 188. If all the values match, the user is authenticated. Thus, at step 250, the authentication server 194 sends an access-accept message to the AAA server 194, instructing the AAA server 196 to authorize the user's access attempt. Finally, at step 252, the AAA server 196 confirms acceptance with the NAS 200.

The present invention can be used to authenticate a user when performing e-commerce transactions. FIG. 7 is a block diagram that illustrates a communication system for authenticating a user when performing e-commerce transactions according to

an exemplary embodiment of the invention. The communication system of FIG. 7 comprises a PLMN 258, a PDN 272, an access network 280, a modem 282, a remote host 284 and a MS 286. The PLMN 258 comprises a BTS 260, a BSC 262, a MSC/VLR 264, a HLR 268, an AuC 270 a SMS-C 266 and a billing system 271. The PDN 272 comprises an authentication server 274, an e-commerce server 276, and a NAS 278. The communication system of FIG. 7 is identical to the communication system of FIG. 1, except the authenticating entity 60 of FIG. 1 is replaced with the e-commerce server 276 and the PLMN 258 has a billing system 271, which is connected to the authentication server 274. With exception to the e-commerce server 276 and the billing system 271, the components of FIG. 7 perform the same function as their corresponding components of FIG. 1, and thus will not be further described herein.

The e-commerce server 276 and the authentication server 274 may be located in different PDNs, so long as a secure data channel exists between them, e.g., IPsec tunnel. Moreover, the remote host 284 may be connected to the PDN 272 through other PDNs, e.g., Internet. In this approach, the authentication, for instance, would be triggered by an e-commerce application that wishes to authenticate the user for a purchase. The e-commerce server 276 would contact the authentication server 274 via a secure packet data connection to request the authentication of the user trying to gain access. The authentication request would include all the relevant payment information, e.g., price, items being purchased. The application may optionally show in the payment information, e.g., price, in the ME (not shown) of the MS 286. After validating a response received from the application, the authentication server 274 would contact a payment server, i.e., the entity handling the charging for the e-commerce application. The payment server can be part of the e-commerce infrastructure or could be integrated with the network billing system 271, or could be an Internet payment provider. If the authentication succeeds, the charging operation is accomplished and the authentication server 274 confirms the payment to the e-commerce server 276 to grant the user access to the requested service or article. Otherwise, an appropriate error condition is sent to the authenticating host. Thus, the user is denied access to the requested service or article.

FIG. 8 is a message sequence chart illustrating a method of authenticating a user when performing an e-commerce transaction according to an exemplary embodiment of

the present invention. According to FIG. 8, the method begins at step 350, where the e-commerce server 276 requests the user's identity. Next, at step 352, the e-commerce application obtains the user identity via a response identity from the User PC 284, e.g., the user is prompted via a display screen of the User PC 284 to input his/her identity. At step 354, the e-commerce server 276 sends the authentication request to the authentication server 274. In addition to the user identity, the authentication request includes all the relevant payment information, e.g., price and items being purchased.

At step 356, the authentication server 274 obtains from the AuC 270 in the PLMN 258 (FIG. 7) a RAND and a SRES pair. Then, at step 358, the authentication server 274 requests the SMS-C 266 to generate a SMS message to request the authentication application in the SIM (not shown) of the MS 286 to authenticate the user. The request contains the RAND obtained from the AuC 270. Optionally, the request may include the price and the items being purchased in order to ensure the integrity of such payment/purchase information.

The authentication server 274 checks the user identity and generates an authentication token. At step 360, the authentication token is sent to the e-commerce server 276. At step 362, the e-commerce server 276 sends an authentication token request to the user via the User PC 284. The User PC 284 displays the authentication token request to the user. At step 364, the SMS-C 266 sends a SMS message including the RAND to the MS 286.

The MS 286 receives the message and forwards it to the authentication application in the SIM (not shown) of the MS 286. The authentication application processes the message and requests the user to enter a PIN code, which may be the SIM's PIN code. The user inputs the PIN code via a keypad of the MS 286 at step 365. The authentication application validates the PIN code. The user has a limited number of re-tries to input the correct PIN code. If the maximum number of consecutive failures is reached, the application prevents the SIM from accepting a PIN code. If the value corresponds to the PIN code stored in the SIM, the authentication application prompts the user for the authentication token.

Still referring to step 365, the user types in the authentication token, which is shown on the display of the User PC 284 (see step 362), using the keypad of the MS 286.

The authentication application applies the appropriate algorithm to the RAND to obtain the SRES. The algorithm utilized in this approach is the GSM A3 authentication algorithm, which obtains the SRES from the RAND and a private key stored in the SIM (step 366). The authentication application requests the MS 286 to send a SMS message containing the authentication token and the SRES to the SMS-C 266.

At step 368, the SMS-C 266 sends the SMS indication message containing the authentication token SRES to the authentication server 274. The authentication server 274 compares the authentication token received to the one sent to the e-commerce application and the SRES to the SRES obtained from the AuC 270. If all the values match, the authentication server 274 could optionally contact a payment server and forward the payment information received from the e-commerce application to the payment server. At step 370, the authentication server 274 generates a charging record (payment information) and transfer it to the billing system 271 of the PLMN 258. Thus, the purchase would be included in the bill corresponding to the wireless subscription of the user.

Once the payment information is communicated, the e-commerce application is informed of the result of the operation. At step 372, the authentication server 274 sends a message to the e-commerce server 276. Finally at step 374, the e-commerce server 276 confirms the operation.

The present invention can be implemented in a communication system that uses Unstructured Supplementary Service Data (USSD). FIG. 9 is a block diagram that illustrates a communication system for USSD according to an exemplary embodiment of the invention. The communication system of FIG. 9 comprises a PLMN 400, a PDN 402, an access network 404, a modem 406, a remote host 408, a MS 410 and a radio link 412. The PLMN 400 comprises a BTS 414, a BSC 416, a MSC/VLR 418, a HLR 420, an AuC 422. The PDN 402 comprises an authentication server 424, an AAA server 426, and a NAS 428. The communication system of FIG. 9 is substantially similar to the communication system of FIG. 1, except the PLMN 400 does not require a SMS-C. In FIG. 9 the AuC 422 is connected to the HLR 420 and the HLR 420 is connected to the authentication server 424. In FIG. 9, the MS 410 user (not shown) and the PLMN 400 operator (not shown) defined application to communicate in a way which is transparent to

the MS 410 and to the intermediate network. The handling of USSD is described in ETS 300 625, which is hereby incorporated by reference.

FIG. 10 is a message sequence chart illustrating a method of handling USSD of the communication system shown in FIG. 9 according to an exemplary embodiment of the present invention. In FIG. 10, The user starts the communication from the User PC 408, which serves as the user's remote access, to the ISP/Intranet (not shown) using a conventional dial-up client application. Once the communication path to the NAS 428 has been established, the set-up process begins. At step 500, the NAS 428 sends an identity request to the User PC 408, requesting the User PC 408 to identify the user. At step 502, the User PC 408 responds to the identity request by sending a response containing the user's identity to the NAS 428. Once the user identity arrives at the NAS 428, at step 504, an access-request (identity) is sent to the AAA server 426. The AAA server 426 checks the identity of the user and forwards the access-request to the authentication server 424 (step 506). At step 508, the authentication server 424 sends a USSD request to the HLR 420. The HLR transmits the USSD request to the MSC/VLR serving the area where the subscriber is currently located. The MSC/VLR receives the request and forwards it to the MS via the BSC and the BTS (not shown in the flow). The authentication server 424 also sends an access-challenge containing the authentication token to the AAA server 426 (step 510).

Next at step 512, the AAA server 426 sends the access-challenge containing the authentication token to the NAS 428. At step 514, the NAS 428 sends a request containing the authentication token to the User PC 408. At step 516, the MSC/VLR 418 sends a USSD request to the MS 410. At step 518, the user inputs the authentication token in the MS 410. At step 520, the MS 410 sends a USSD response containing the authentication token the MSC/VLR 418.

At step 522 the User PC 408 sends a response message to the NAS 428. Then, at step 524 the NAS 428 sends an access-request containing the user identity and the response message to the AAA server 426. The AAA server 426 sends the access-request containing the user identity and the response request to the authentication server 424 (step 526). At step 528, the HLR 420 sends a USSD response containing the authentication token to the authentication server 424. At step 530 the authentication server sends an

access-accept message to the AAA server 426. Finally, at step 532, the AAA server 426 sends the access-accept message to the NAS 428.

The present invention can be implemented in a communication system that uses the WAP. The WAP specifies an application framework as well as network protocols for wireless devices. The WAP model is similar to the World Wide Web (WWW), being optimized to match the characteristics of the wireless environment. The WAP architecture and protocols are specified in the corresponding WAP Forum specifications, e.g., WAP Architecture, April 30, 1998, wherein the latest version is WAP specification suite 1.1.

FIG. 11 is a block diagram that illustrates a communication system for WAP according to an exemplary embodiment of the present invention. The communication system comprises a PLMN 600, a PDN 602, an access network 604, a remote host 606, a MS 608 containing a WAP browser (not shown), and a radio link 610. The PDN 602 comprises an authenticating entity 614, an authentication server 616, a NAS 618 and a WAP server 620.

The PLMN 600 may be constructed according to the GSM standards. The PLMN 600 may comprise a WAP Gateway 612. The WAP Gateway 612 maybe connected to the WAP server 620 via communication link 626. The WAP server 620 maybe connected to the authentication server 616 via communication link 628. In FIG. 11, the MS user and the authentication application in the WAP Server 620 communicate according to the WAP specifications defined by the WAP Forum.

FIG. 12 illustrates a method of authenticating a user in the communication system shown in FIG. 11 according to an exemplary embodiment of the present invention. In FIG. 12, the user requests a service that requires authentication. The method begins at step 700 where the authenticating entity 614 sends an identity request to the User PC 606 to identify the user. At step 702, the User PC 606 responds to the identity request by sending a response containing the user's identity to the authenticating entity 614. At step 704, the authenticating entity 614 sends an access-request to the authentication server 616. At step 706, the authentication server 616 sends an authentication token to the authenticating entity 614. The authentication server 616 also sends an authentication request to the authentication application within the WAP server 620 (step 708).

At step 710, the authenticating entity 614 sends the authentication token to the User PC 606. The WAP server 620 pushes the request through the WAP gateway 612 to the MS 608 (steps 712 and 714).

At step 716, the user inputs the authentication token in the MS 608. At steps 718 and 720, the MS 608 sends a response containing the authentication token through the WAP gateway 612 to the WAP server 620. At step 722, the WAP server 620 sends a response containing the authentication token to the authentication server 616.

Finally, at step 724, the authentication server sends an access accept message to the authenticating entity 614.

It will be appreciated by those of ordinary skill in the art that the present invention can be embodied in other specific forms without departing from its essential character. Thus, the embodiments described herein should therefore be considered in all respects to be illustrative and not restrictive.

WHAT IS CLAIMED IS:

1. A method of authenticating a user requesting access to a packet data network (PDN), comprising the steps of:

(a) receiving an access request to the PDN;

(b) generating an authentication token;

(c) sending the authentication token to the user from the PDN via an access network over an unsecured or secured communication link;

(d) interrogating the user from the PDN for the authentication token via a secured communication link over a public land mobile network (PLMN)

(e) sending the authentication token received by the user to the PDN via the secured communication link over the public land mobile network (PLMN); and

(f) comparing the authentication token of step (c) to the authentication token of step (e) to determine whether the user is granted access to the PDN.

2. The method of claim 1, wherein the user is granted access to the PDN if the authentication token of step (c) matches the authentication token of step (e).

3. The method of claim 1, wherein the user is denied access to the PDN if the authentication token of step (c) does not match the authentication token of step (e).

4. The method of claim 1, further comprising the step of utilizing an authenticating entity to send a request to an authentication server, wherein the authentication server checks the user's identity.

5. The method of claim 4, further comprising the step of utilizing the authenticating entity to generate the authentication token.

6. The method of claim 5, further comprising the step of utilizing the authentication server to send the authentication token to the PDN.

7. The method of claim 6, wherein the authentication server compares the authentication token of step (c) to the authentication token of step (e).

8. The method of claim 7, wherein step (e) further comprises utilizing a mobile station to send the authentication token to the PDN via the PLMN.

9. The method of claim 8, further comprising the step of entering at least one of a Personal Identification Number (PIN) code or the authentication token in the mobile station.

10. The method of claim 8, further comprising the step of entering at least one of a Personal Identification Number (PIN) code or the authentication token in a remote host, wherein the mobile station is connected to the remote host via a wireline or a wireless connection to transmit the PIN code or the authentication token from the remote host to the mobile station via the wireline or the wireless connection.

11. The method of claim 8, further comprising the step of sending automatically a Personal Identification Number (PIN) code stored at a remote host to the mobile station.

12. The method of claim 8, further comprising the step of sending the authentication token from the PDN to a remote host, wherein the remote host automatically sends the authentication token to the mobile station.

13. The method of claim 8, further comprising the step of performing end-to-end encryption of information being transferred between the mobile station and the authentication server via the PLMN.

14. The method of claim 13, further comprising the steps of utilizing the authentication server to contain an encryption key generation algorithm or formula and utilizing the encryption key generation algorithm or formula to calculate an encryption

key per communication session between the mobile station and the authentication server via the PLMN.

15. The method of claim 13, further comprising the steps of utilizing the mobile station to contain an encryption key generation algorithm or formula and utilizing the encryption key generation algorithm or formula to calculate an encryption key per communication session between the mobile station and the authentication server via the PLMN.

16. The method of claim 13, further comprising the steps of utilizing the authentication server to contain an encryption algorithm and applying the encryption algorithm to information being transferred between the mobile station and the authentication server via the PLMN.

17. The method of claim 13, further comprising the steps of utilizing the mobile station to contain an encryption algorithm and applying the encryption algorithm to information being transferred between the mobile station and the authentication server via the PLMN.

18. The method of claim 8, further comprising the step of challenging of the user's individual authentication key stored in the mobile station from the authentication server when communicating through the PLMN.

19. The method of claim 18, further comprising the steps of utilizing the authentication server to compare the result of challenging the user's authentication key, and, together with the authentication token check, determining whether the user is granted access to the PDN.

20. The method of claim 18, further comprising the step of utilizing the mobile station to contain an authentication algorithm and to generate responses to the challenge that may be sent to the authentication server together with the authentication token

through the PLMN.

21. The method of claim 1, further comprising the step of performing end-to-end encryption of information being transferred between the user and the PDN once the user has been granted access to the PDN.

22. The method of claim 21, further comprising the steps of utilizing the authentication server to contain an encryption key generation algorithm or formula and utilizing the encryption key generation algorithm or formula to calculate an encryption key per communication session between the user and the PDN via the access network.

23. The method of claim 21, further comprising the steps of utilizing a mobile station to contain an encryption key generation algorithm or formula and utilizing the encryption key generation algorithm or formula to calculate an encryption key per communication session between the user and the PDN via the access network.

24. The method of claim 21, further comprising the step of utilizing a mobile station to transfer an encryption key to a remote host for further usage to encrypt the information being transferred between the user and the PDN once the user has been granted access to the PDN.

25. The method of claim 21, further comprising the steps of utilizing the PDN to contain an encryption algorithm and applying the encryption algorithm to information being transferred between the user and the PDN once the user has been granted access to the PDN.

26. The method of claim 21, further comprising the steps of utilizing a remote host to contain an encryption algorithm and applying the encryption algorithm to information being transferred between the user and the PDN once the user has been granted access to the PDN.

27. A communication system for authenticating a user requesting access to a packet data network (PDN), comprising:

a) a Public Land Mobile Network (PLMN) connected to the PDN;

b) a remote host connected to the PDN via an access network; and

c) a mobile station coupled to the PLMN via a wireless link, wherein in response to receiving a user request to the PDN, the PDN generates and sends an authentication token over an unsecured or secured communication link to the user via the access network and the remote host, the user sends the authentication token back to the PDN over the PLMN, wherein the PDN compares the authentication tokens to determine whether to grant the user access to the PDN.

28. The communication system of claim 27, wherein the PLMN further comprises:

a base transceiver station connected to a base station controller;

a mobile switching center/visited location register connected to both a short message service center and the base station controller; and

a home location register connected to an authentication center.

29. The communication system of claim 28, wherein the remote host is connected to the network access server via the access network.

30. The communication system of claim 29, wherein the short message service center is connected to an authentication server.

31. The communication system of claim 30, wherein the authentication server is connected to the home location register.

32. The communication system of claim 31, wherein the authentication server is connected to a Wireless Application Protocol (WAP) server.

33. The communication system of claim 32, wherein the PDN further

comprises an authenticating entity connected to both the authentication server and a network access server.

34. The communication system of claim 31, wherein the PDN further comprises:

an authentication, authorization and accounting (AAA) server connected to the authentication server; and

a network access server connected to the AAA server.

35. The communication system of claim 34, wherein the authentication server has the ability to connect to various PLMN interfaces to use at least one of Short Message Service, Unstructured Supplementary Service Data or Wireless Application Protocol wireless technologies.

36. The communication system of claim 34, wherein the authentication server is connected to the PLMN via an intermediate gateway system.

37. The communication system of claim 31, wherein the PDN further comprises:

an e-commerce server connected to both the network access server and the authentication server; and

a billing system connected to the authentication server.

38. The communication system of claim 37, wherein the mobile station comprises:

mobile equipment; and

a subscriber identification module (SIM).

39. The communication system of claim 38, wherein the SIM further comprises, a SIM operative system, a GSM part, a SIM Application Toolkit, and an authentication application, wherein the SIM operative system together with the SIM

Application Toolkit provide the proper environment for the authentication application to function and communicate with the authentication server.

40. The communication system of claim 39, wherein messages transferred between the authentication application and the authentication server are encrypted.

41. A method of authenticating a user when performing an e-commerce transaction comprising the steps of:

(a) receiving an access request to a Packet Data Network (PDN) to perform the e-commerce transaction;

(b) generating an authentication token;

(c) contacting a payment server that handles the changing for an e-commerce application;

(d) sending the authentication token to the user from the PDN via an access network over an unsecured or secured communication link;

(e) sending the authentication token received by the user to the PDN via a secured communication channel over a public land mobile network (PLMN); and

(f) comparing the authentication token of step (d) to the authentication token of step (e) to determine whether the user performing the e-commerce transaction is authenticated.

42. The method of claim 41, wherein an authentication server communicates with the payment server to charge the user for the e-commerce transaction.

43. The method of claim 42, wherein billing information is sent to a billing system.

44. A communication system for authenticating a user requesting access to a Packet Data Network (PDN), comprising:

(a) means for receiving an access request to the PDN;

(b) means for generating an authentication token;

(c) means for sending the authentication token to the user from the PDN via an access network over an unsecured or secured communication link;

(d) means for sending the authentication token received by the user to the PDN via a secure communication channel over a public land mobile network (PLMN); and

(e) means for comparing the authentication token of step (c) to the authentication token of step (d) to determine whether the user is granted access to the PDN.

45. The communication system of claim 44, further comprising:

(f) means for generating a session key per communication session with a mobile station via the PLMN;

(g) means for generating the session key per communication session with a remote host via an access network, once the user has been granted access to the PDN;

(h) means for challenging the user's individual authentication key stored in the mobile station via the PLMN;

(i) means for checking the result of the challenge to the user's individual key and, together with checking of the authentication token, determine whether the user is granted access to the PDN;

(j) means for applying an encryption algorithm to information being interexchanged with the mobile station via PLMN; and

(k) means for applying the encryption algorithm to the information being interexchanged with the remote host via the access network, once the user has been granted access to the PLMN.

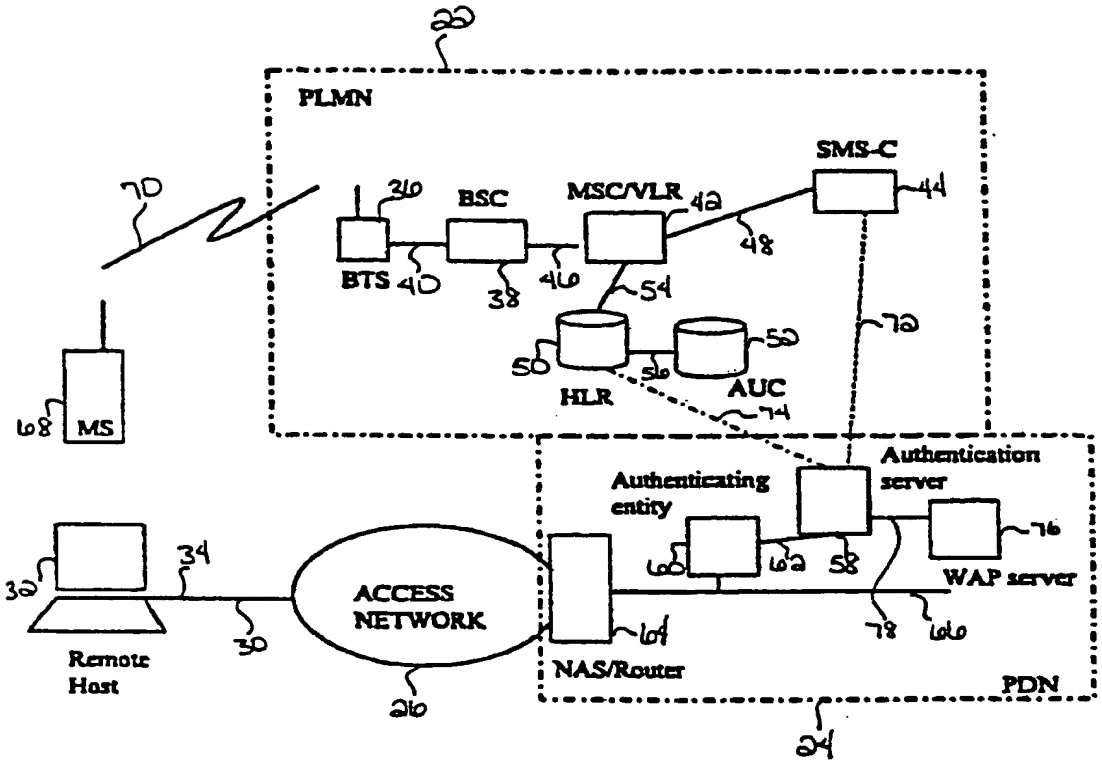


FIG. 1

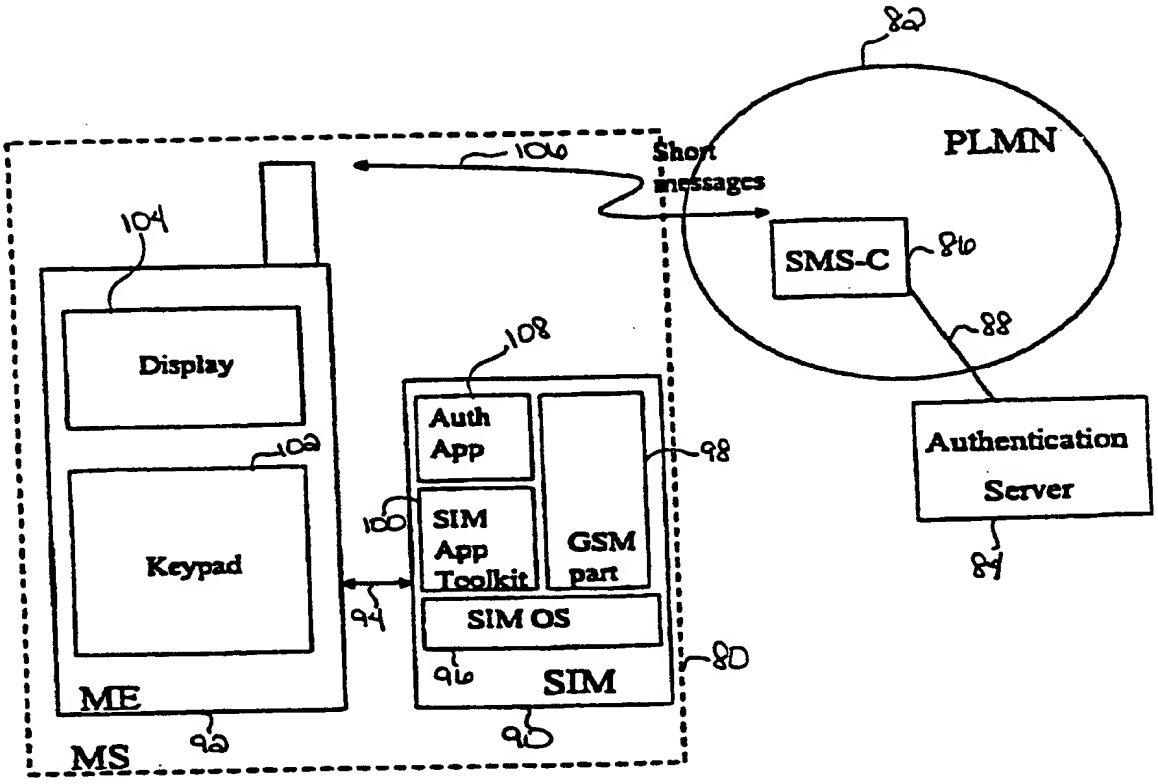


FIG. 2

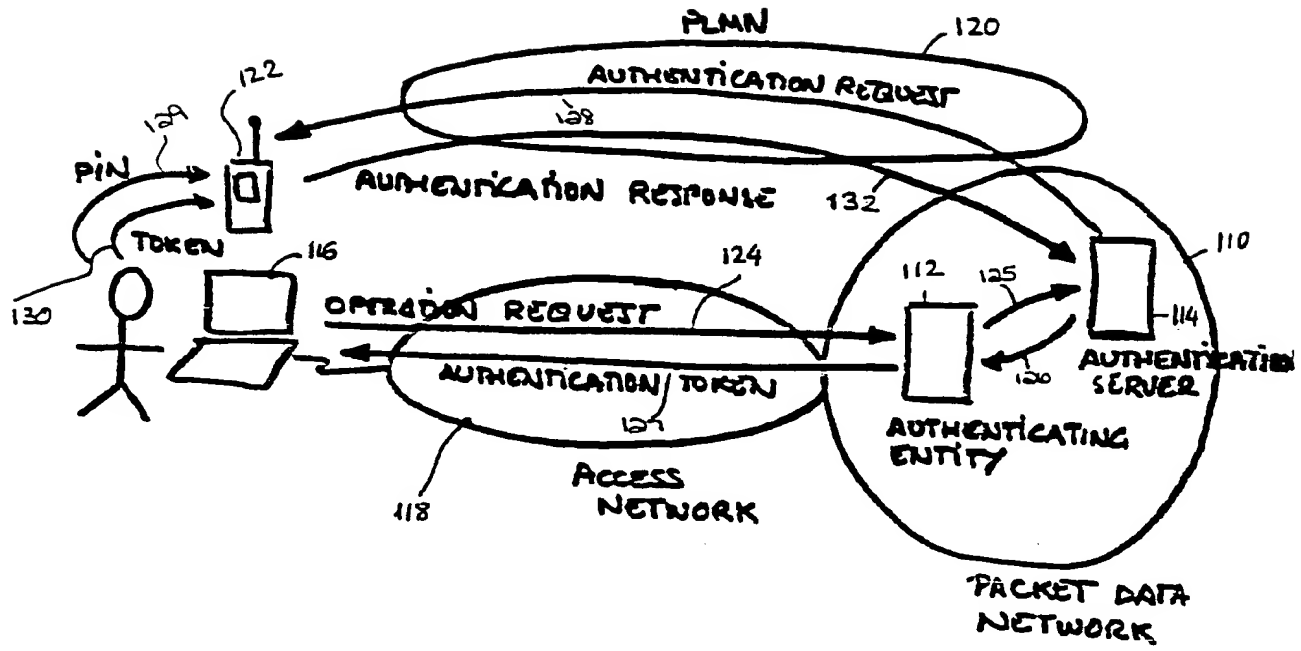


FIG.3

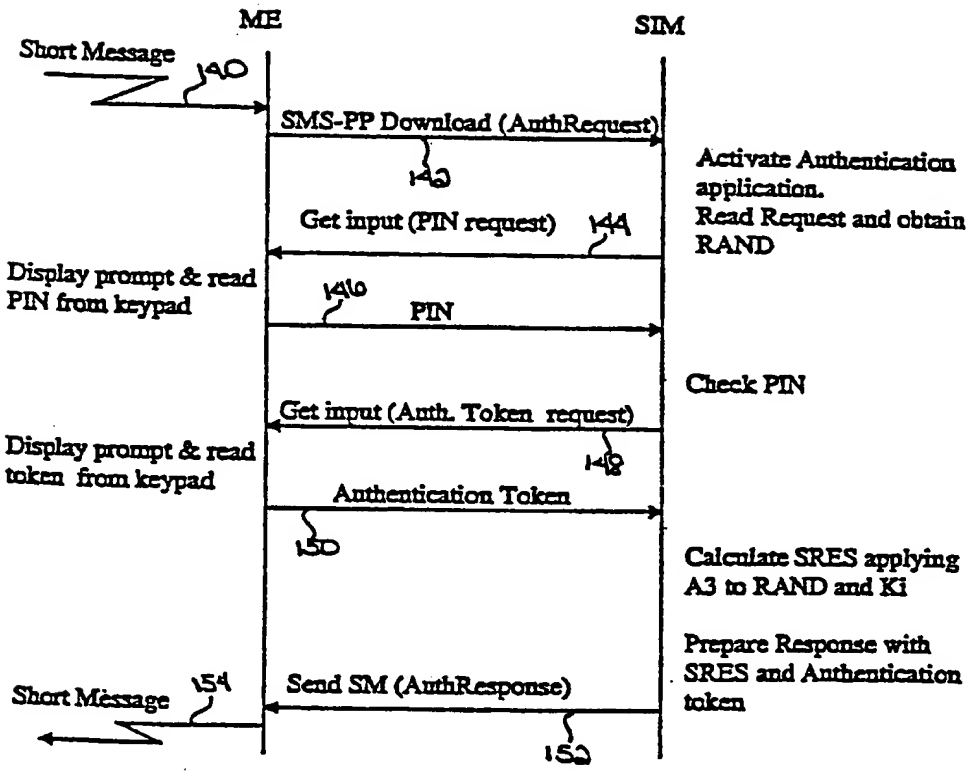


FIG. 4

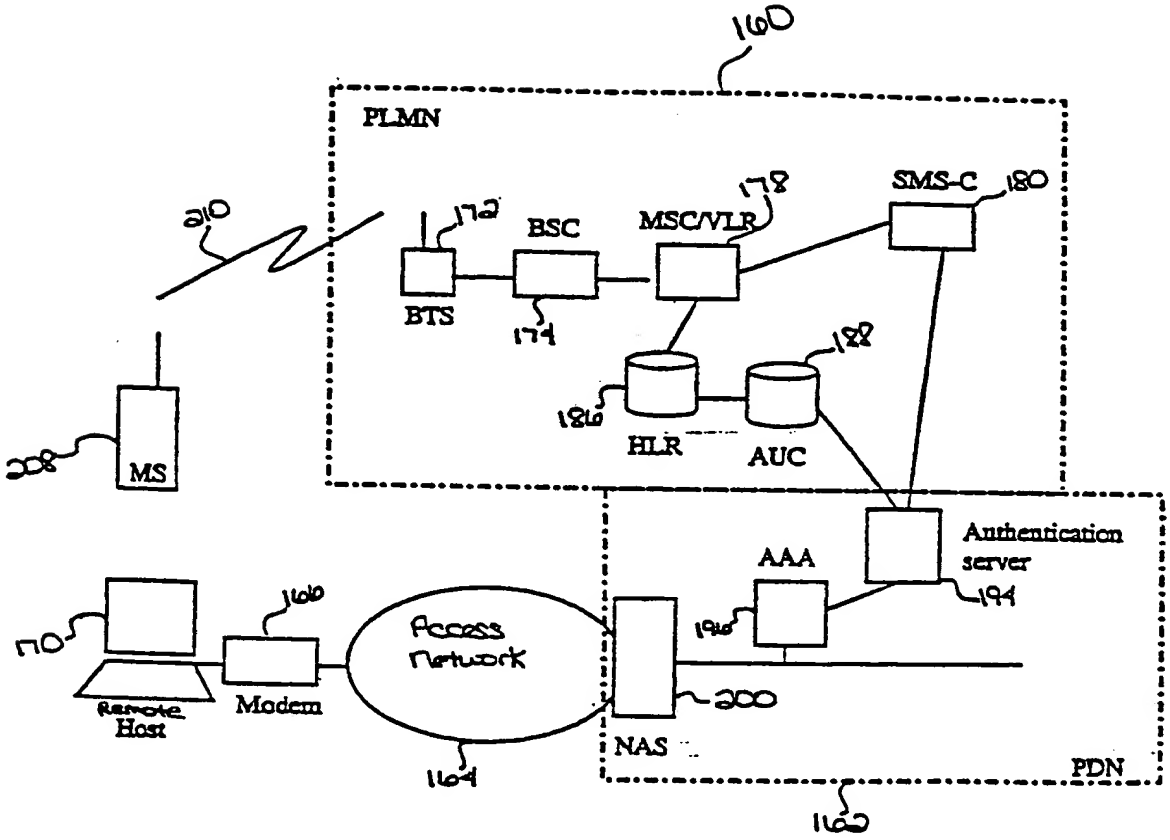


FIG.5

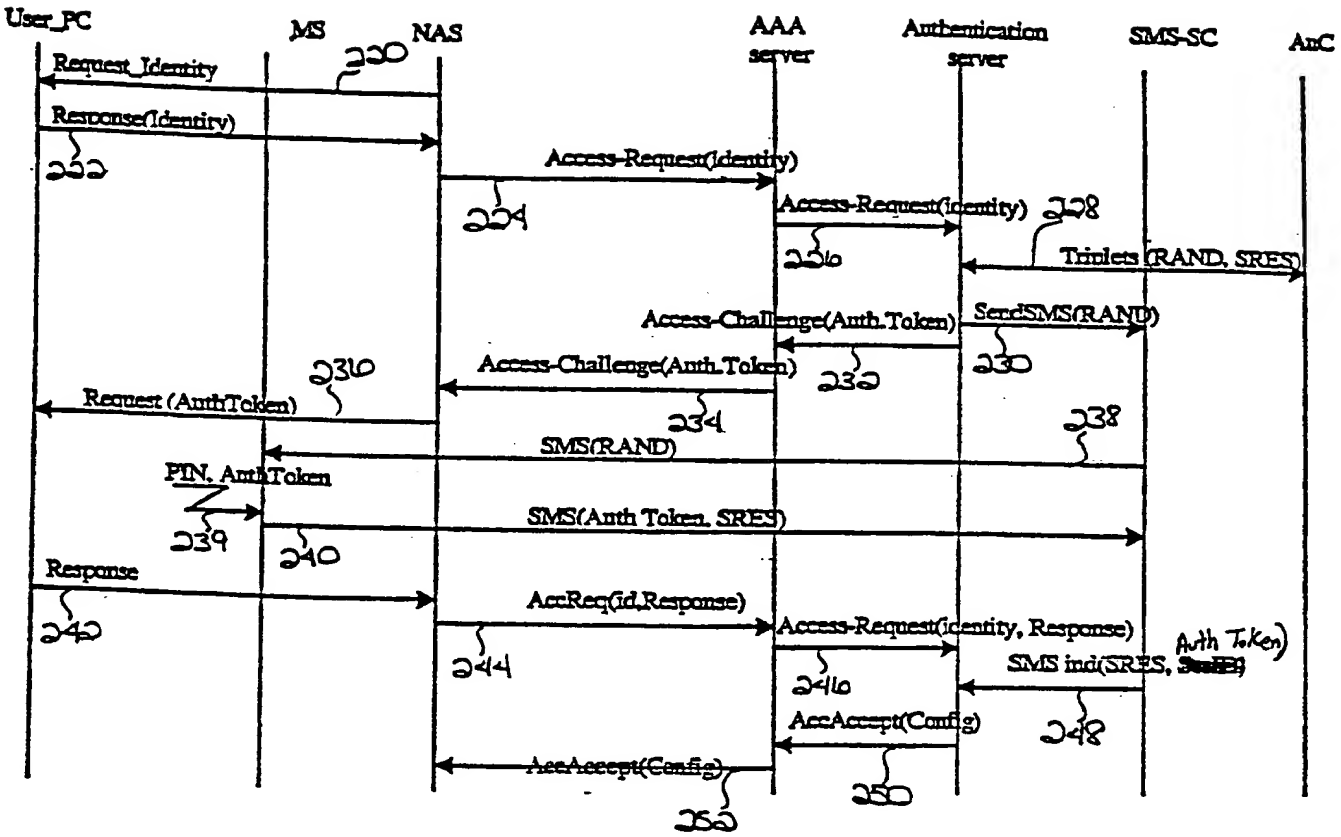


FIG. 6

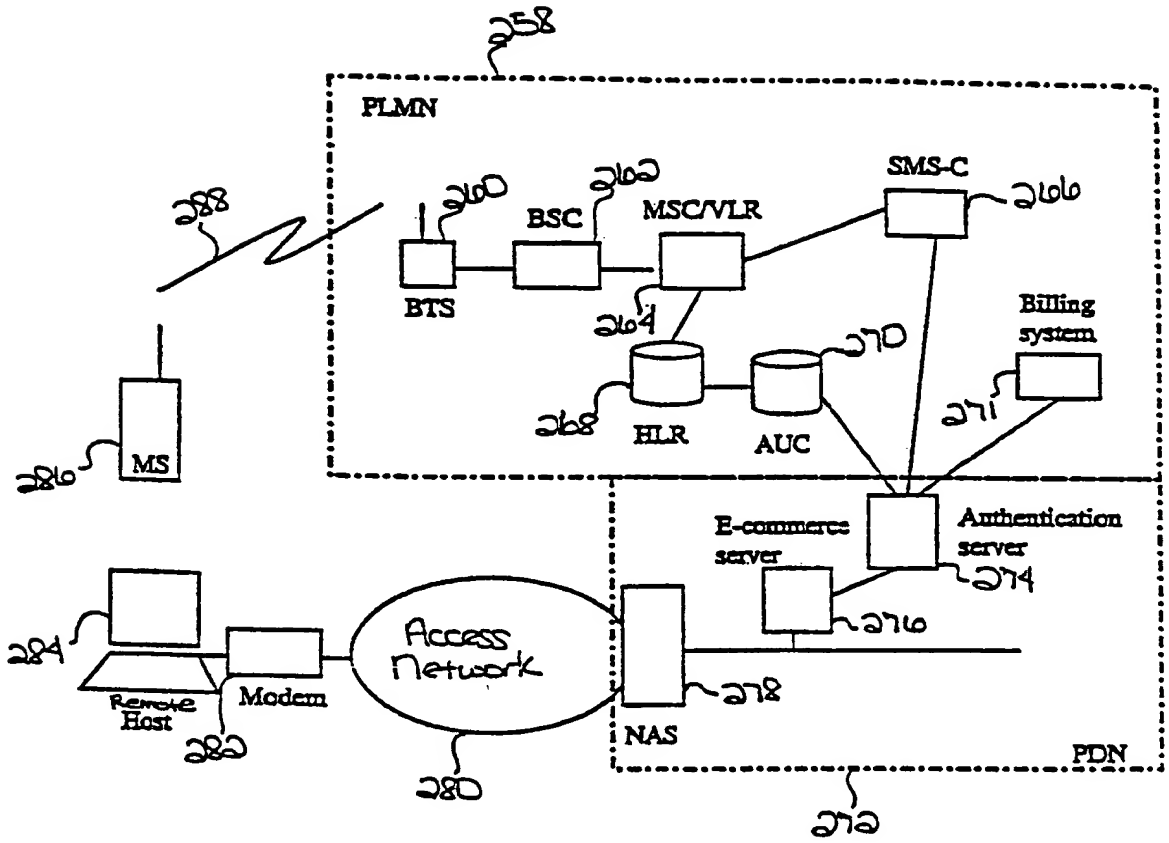


FIG.7

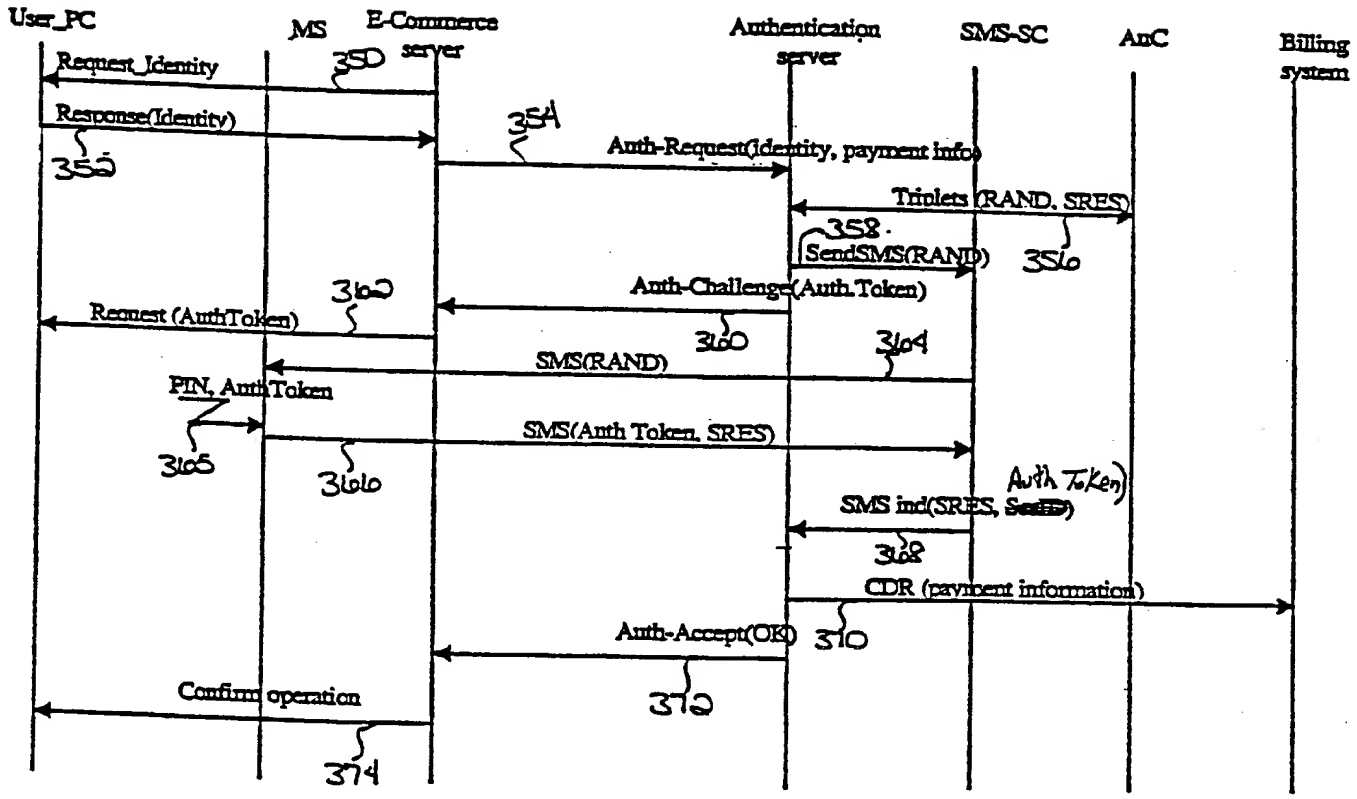


FIG.8

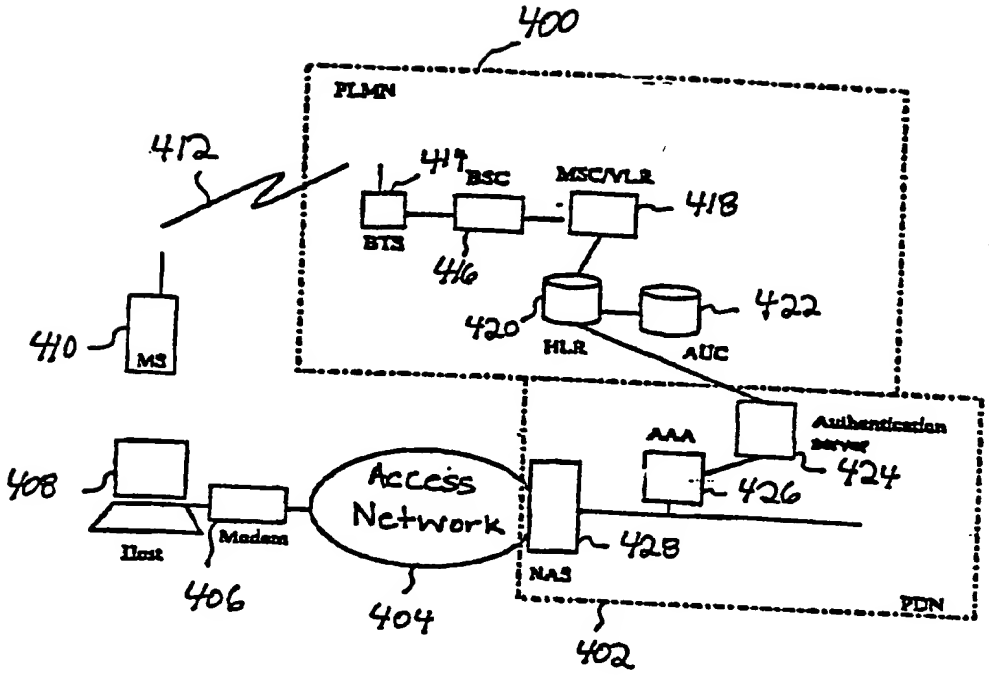


FIG. 9

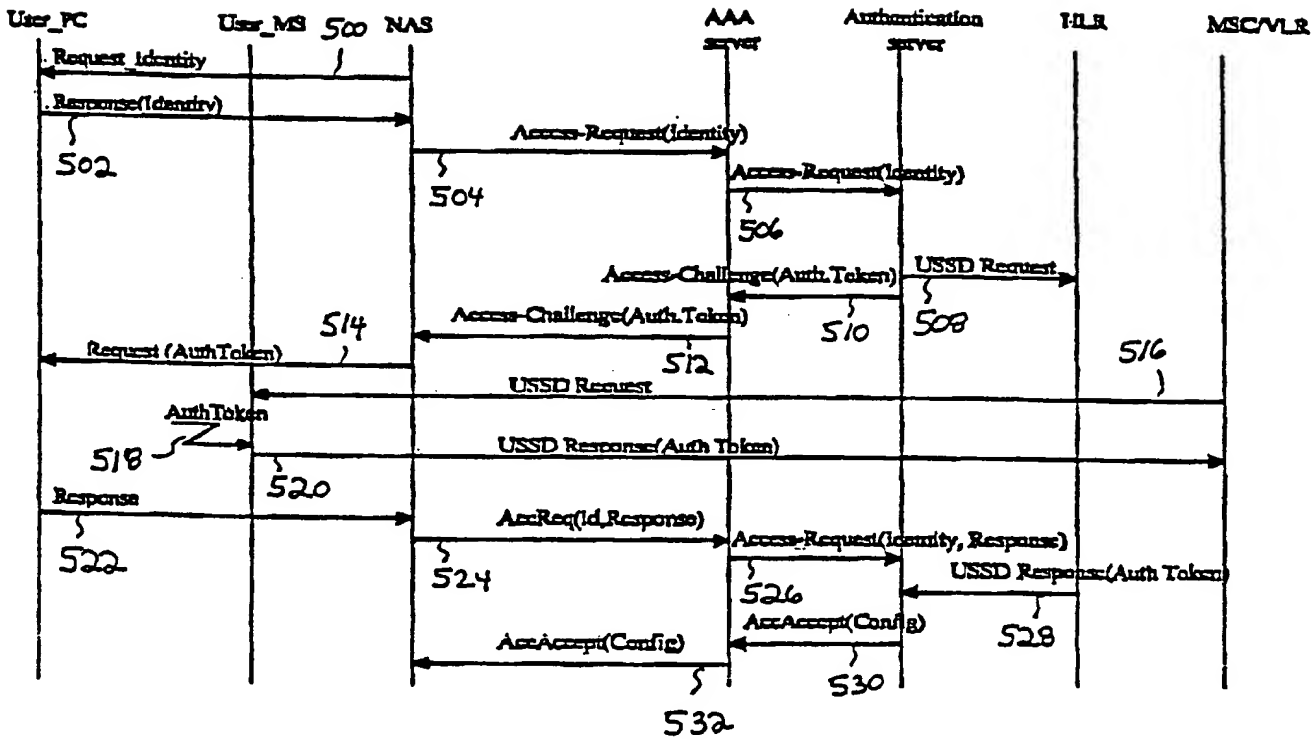


FIG. 10

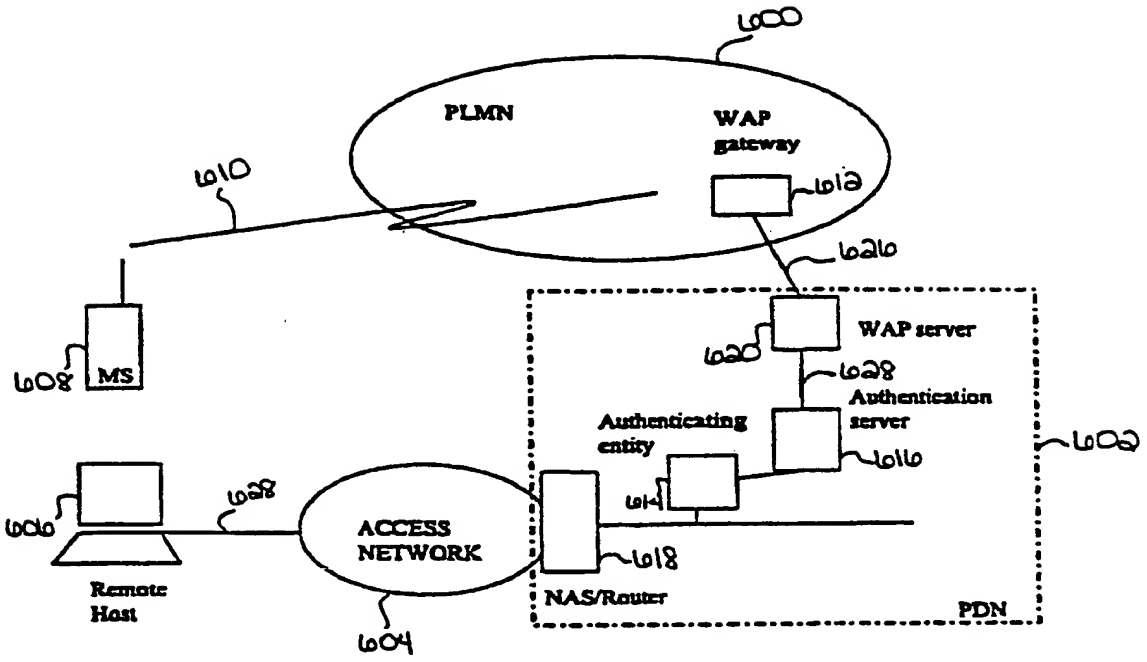


FIG. 11

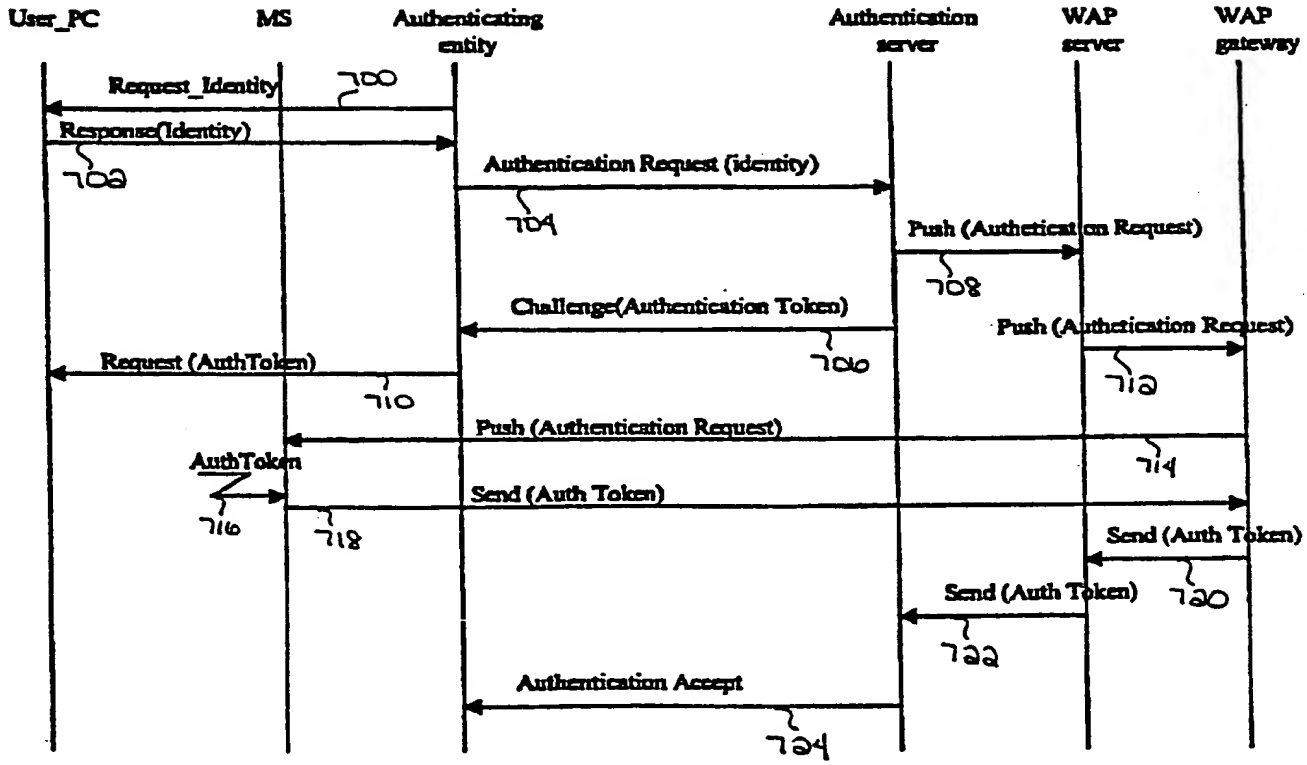


FIG. 10

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/SE 00/01673

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropnate, of the relevant passages	Relevant to claim No.
X	US 5 668 876 A (FALK JOHAN PER ET AL) 16 September 1997 (1997-09-16) column 1, line 66 -column 2, line 21 column 2, line 66 -column 6, line 55 column 8, line 33 - line 40 figures 1-3	1-10, 13-20, 27,41,44
A	WO 99 23617 A (KREMER GILLES ;CHANUDET PATRICK (FR)) 14 May 1999 (1999-05-14) page 2, line 12 -page 3, line 15 page 6, line 19 -page 7, line 29 page 10, line 5 -page 11, line 6 page 14, line 12 -page 21, line 3 page 29, line 30 -page 30, line 3 page 35, line 8 - line 33 page 41, line 3 -page 42, line 26 figures 1-4,12	1-45

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 December 2000	12/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Barel, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

.. .ormation on patent family members

Interr ıal Application No
PCT/SE 00/01673

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5668876 A	16-09-1997	AU 692881 B	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A	04-01-1996
		EP 0766902 A	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
		WO 9600485 A	04-01-1996
WO 9923617 A	14-05-1999	FR 2771875 A	04-06-1999
		AU 1158899 A	24-05-1999
		EP 1050025 A	08-11-2000